Exhibit 17

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

ANAS EHADY, et al.,	)	
Plaintiffs,	)	
v.	)	Case No. 1:16-cv-375
CHARLES H. KABLE, et al.	)	
Defendants.	)	

DECLARATION OF TIMOTHY P. GROH
SUBMITTED IN CAMERA, EX PARTE

I, Timothy P. Groh, hereby declare as follows, pursuant to 28 U.S.C. § 1746:

1. (U) I am the Deputy Director for Operations of the Terrorist Screening Center ("TSC") and have been in this position since May 2016. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since February 1996 and have served in a variety of criminal investigative, counterterrorism, and senior management positions. In my capacity as the Deputy Director for Operations of the TSC, I supervise nine units and approximately three hundred individuals (including both government employees and contractors). I am responsible for the overall operations of the TSC, including building and maintaining the Terrorist Screening Database (TSDB), managing encounters, and sharing intelligence with domestic and foreign partners.

2. (U) I submit this declaration in support of the government's opposition to plaintiffs' motion to compel production of various documents and interrogatory responses over which the government has asserted the law enforcement privilege, in *Elhady v. Kable*, 16-cv-375

(E.D.V.A.). The purpose of this declaration is to assist the Court in evaluating the government's claim of law enforcement privilege, by describing the U.S. government's consolidated terrorist watchlist, explaining how that list is created and used, and clarifying why detailed information pertaining to watchlisting (including whether an individual is in the TSDB) cannot be publicly disclosed.

3. (U) The matters stated herein are based on my personal knowledge, my background, training and experience relating to terrorist watchlisting and counterterrorism investigations, and my review and consideration of information available to me in my official capacity, including information furnished by FBI and TSC personnel in the course of their official duties; my conclusions have been reached in accordance therewith.

4. (U) I have personally reviewed the information contained in documents, or samples of document sets of cumulative information where sampling was appropriate, sought by Plaintiffs in their motion to compel.

5. (U) Each paragraph in this declaration is marked with letters indicating the level of classification applicable to that paragraph. Paragraphs marked with a "U" are unclassified. Paragraphs designated "U//LES" are considered to be "Unclassified//Law Enforcement Sensitive." Paragraphs designated "U//LES//SSI" are considered to be "Unclassified//Law Enforcement Sensitive//Sensitive Security Information." All SSI markings were made in consultation with TSA.

6. (U) This declaration was prepared and executed in connection with a State Secrets Privilege declaration pertaining to many of the same documents and should be read in connection with that declaration. Each argument in that declaration would also support an assertion of Law Enforcement Privilege over the same documents.

I. (U) OVERVIEW OF THE CONSOLIDATED U.S. TERRORIST WATCHLIST

7. (U) The TSDB is the federal government's consolidated terrorist watchlist. The TSDB in general contains names and other identifying information (e.g., dates of birth, photographs, iris scans, and fingerprints) of individuals known or reasonably suspected to be or to have been engaged in conduct constituting, in preparation for, in aid or in furtherance of, or related to terrorism and/or terrorist activities. The TSDB does not contain the underlying classified intelligence or other derogatory information that is the basis for the individual's inclusion in the database. Segregating the identifying information in this way facilitates information-sharing among U.S. Government watchlisting and screening agencies.

8. (U) Nonetheless, much of the information in the TSDB is derived from classified or other legally restricted information. As a result, disclosure of TSDB information for any purpose other than an authorized watchlisting function must be approved by the originator of the underlying information.

9. (U) The TSDB was created and is maintained by TSC, a federal multi-agency center administered by the FBI. The FBI is the agency responsible for submitting nominations of individuals suspected of links to domestic terrorism for inclusion in the TSDB. The National Counterterrorism Center (NCTC) is the agency responsible for submitting nominations of individuals suspected of links to international terrorism for inclusion in the TSDB and serves as the central agency for gathering and analyzing all intelligence obtained by the U.S. Government pertaining to international terrorism.

10. (U) Upon receipt of this identity information, TSC reviews the nominations received from the FBI and/or NCTC, as well as the underlying derogatory information maintained by those entities and information from other sources, to determine whether an individual meets the

criteria for inclusion in the TSDB. Inclusion in the TSDB generally requires a determination that there is a reasonable suspicion that the individual is engaged, has been engaged, or intends to engage in conduct constituting, in preparation for, in aid or in furtherance of, or related to, terrorism and/or terrorist activities. That determination must be based on articulable intelligence or information, taken together with any rational inferences that can be drawn from that intelligence or information. The determination must consider the totality of the circumstances.

11. (U) The TSDB also includes identifying information of some individuals who do not meet the reasonable suspicion standard, but only for the limited purpose of supporting specific screening functions of the Department of Homeland Security and the Department of State (such as determining eligibility for immigration to the United States) and which are exported to those agencies only for these purposes. In other words, these individuals are not considered "known or suspected terrorists" (KSTs) and are not screened as such. As a result, any U.S. person who is in the TSDB pursuant to an exception to the reasonable suspicion standard would not generally be subject to heightened aviation security screening at airports. In order to maintain the effectiveness of these special screening functions, details regarding the method by which individuals are identified for watchlisting exceptions must not be disclosed and are properly categorized as law enforcement sensitive.

12. (U) A subset of persons listed in the TSDB are placed on the No Fly List when the TSC determines that an individual, in addition to meeting the reasonable suspicion standard, poses at least one of the following: (a) a threat of committing an act of international terrorism (as defined in 18 U.S.C. § 2331(1)) or domestic terrorism (as defined in 18 U.S.C. § 2331(5)) with respect to an aircraft (including a threat of air piracy, or a threat to airline, passenger, or civil aviation security); (b) a threat of committing an act of domestic terrorism (as defined in 18

U.S.C. § 2331(5) with respect to the homeland; (c) a threat of committing an act of international terrorism (as defined in 18 U.S.C. § 2331(1)) against any U.S. government facility abroad and associated or supporting personnel, including U.S. embassies, consulates and missions, military installations (as defined by 10 U.S.C. § 2801(c)(4)), U.S. ships, U.S. aircraft, or other auxiliary craft owned or leased by the U.S. Government; or (d) a threat of engaging in or conducting a violent act of terrorism and who is operationally capable of doing so. Individuals on the No Fly List are prohibited from boarding a U.S. commercial aircraft or from flying into, out of, or over United States airspace.

13. (U) Another subset of persons in the TSDB is included in the Selectee List, which identifies passengers who may be subject to additional security screening before being permitted to board an aircraft. TSC places individuals on the Selectee List if it determines they meet the reasonable suspicion standard applicable to known or suspected terrorists and also satisfy additional specific criteria.

14. (U) Several federal agencies use information from the TSDB for a variety of national security and law enforcement screening and vetting purposes. For example, U.S. Customs and Border Protection receives information from the TSDB and may rely on that information when inspecting individuals at U.S. ports of entry. The Transportation Security Administration (TSA) also uses information in the TSDB in implementing aviation security procedures.

15. (U) TSC and the nominating agencies seek to ensure the continuing accuracy of the information in the TSDB. An intelligence or law enforcement agency that nominated an individual to the TSDB because of suspected ties to international terrorism is expected to promptly notify the NCTC of any information that might require modification or deletion of an individual from the TSDB, and the NCTC must then transmit that information to TSC. The FBI

is likewise required to promptly notify TSC if it receives information suggesting the need to modify or delete a record from the TSDB with respect to an individual suspected of links to domestic terrorism. In addition, records in the TSDB are regularly reviewed to verify that there is adequate support for continued inclusion in the database. Without current, reliable and accurate information in the TSDB, the purpose of sharing information in order to protect the national security of the United States would be defeated. Thus, these regular reviews are rigorous to ensure the integrity of the TSDB.

16. (U) The "Overview of the U.S. Government's Watchlisting Process and Procedures," ("Overview Document") produced to Plaintiffs at Elhady-FBITSC-001947-001956, contains additional information about the process for nomination of individuals to the TSDB, use of the TSDB information by domestic agencies, quality assurance measures to ensure that information in the TSDB is thorough, accurate, and current, and the available process for redress requests. It is the result of a lengthy interagency process to publicly disclose as much information about the U.S. government terrorism watchlisting process and procedures as the watchlisting community determined could be made public without compromising national security and law enforcement interests. The Overview Document was prepared for the purpose of more fully and clearly informing the public of watchlisting processes.

II. (U) SCOPE OF PRIVILEGE ASSERTED

17. (U) I submit this declaration to assert and support a claim of law enforcement privilege over law enforcement sensitive information contained in documents listed in Exhibit K to Plaintiffs' motion to compel or otherwise described in and sought by Plaintiffs' motion to compel. Based upon my review of this matter, and for the reasons explained below, I hereby formally assert the law enforcement privilege, on behalf of the FBI and TSC, over the documents listed in Exhibit K and other information described in and sought by Plaintiffs' motion to

compel. I will explain below the types of law enforcement sensitive information Plaintiffs seek to compel, as well as the harms that would result from the disclosure of this sensitive law enforcement information.

18. (U) The sensitive law enforcement information Plaintiffs seek to compel falls into one or more of the following eight categories:

a. Nominations and Placement

b. Information Sharing (including Foreign Partner Information)

c. Screening and Encounters

d. Redress Policy Documents

e. Identities and Contact Information

f. Audit Documents

g. TSDB Statistics

h. TSDB Status

19. (U) As discussed more fully below, disclosure of this information could reasonably be expected to risk circumvention of the law and to cause harm to law enforcement and counterterrorism investigations, as disclosure of these documents would reveal sensitive, closely-guarded information about the internal workings of the watchlisting process, including the type, quality, and amount of information needed to watchlist an individual, as well as how this information is received, vetted, and disseminated to foreign and domestic partners. It would further enable those seeking to do harm to take evasive measures in order to avoid detection at various points in the watchlisting process, or potentially even enhance their efforts to test the strengths and weaknesses in the process at these various points.

A. (U) Nominations and Placement

20. (U) While TSC has publicly disclosed certain aspects of the watchlisting enterprise (by way of the Overview Document, TSC FAQ, and other documents, which have been provided to plaintiffs), the specific policies and procedures concerning placement of individuals in the TSDB or its subsets, including detailed guidance as to how an analyst should treat specific situations and specific pieces of intelligence in evaluating whether a nominated subject satisfies a criteria for inclusion in the TSDB or its subsets, have not been publicly revealed. Disclosure of this information would provide terrorists and their associates with a roadmap of the specific techniques and procedures by which the United States gathers, evaluates, analyzes, and shares information concerning known or suspected terrorists, and by which Defendants utilize the TSDB and the No Fly and Selectee Lists to protect national security. Release of this information thus could reasonably be expected to risk circumvention of the law and cause harm to national security.

21. (U) Documents relating to nominations and placement include, without limitation, documents listed in Plaintiffs' Exhibit K[1] and the following specific information sought by

[1] (U) TSCA0001; TSCA0002; TSCA0003; TSCA0004; TSCA0005; TSCA0006; TSCA0007; TSCA0008; TSCA0009; TSCA0010; TSCA0011; TSCA0012; TSCA0013; TSCA0014; TSCA0015; TSCA0019; TSCB0002 (Elhady-FBITSC-PRIV00002); TSCB0004 (Elhady-FBITSC-PRIV00004-00018); TSCB0005 (Elhady-FBITSC-PRIV00019-00070); TSCB0006 (Elhady-FBITSC-PRIV00071-00077); TSCB0007 (Elhady-FBITSC-PRIV00078-00130); TSCB0012 (Elhady-FBITSC-PRIV00320-00346); TSCB0013 (Elhady-FBITSC-PRIV00347-00354); TSCB0014 (Elhady-FBITSC-PRIV00355-00356); TSCB0016 (Elhady-FBITSC-PRIV00396-00423); TSCB0017-0037 (Elhady-FBITSC-PRIV00424-00444); TSCB0002 (Elhady-FBITSC-PRIV00002); TSCC0010 (Elhady-FBITSC-PRIV002867-002989); TSCC0011 (Elhady-FBITSC-PRIV002990-003098); TSCD0006 (Elhady-FBITSC-PRIV003144); TSCD0009 (Elhady-FBITSC-PRIV003185); TSCC0011 (Elhady-FBITSC-PRIV002990-003098); TSCD0012 (Elhady-FBITSC-PRIV003228-003248); TSCD0013 (Elhady-FBITSC-PRIV003249-003257); TSCD0014 (Elhady-FBITSC-PRIV003258-003266); TSCD0015 (Elhady-FBITSC-PRIV003267-003268); TSCD0016 (Elhady-FBITSC-PRIV003269-003290); TSCD0018 (Elhady-FBITSC-PRIV003294-003303); TSCD0022 (Elhady-FBITSC-PRIV003473-003487); TSCD0023 (Elhady-FBITSC-PRIV003488-003515); TSCD0024 (Elhady-FBITSC-PRIV003516-003518); TSCD0026 (Elhady-FBITSC-PRIV003520-003535); TSCD0027 (Elhady-FBITSC-PRIV003536-003546); TSCD0029 (Elhady-FBITSC-PRIV003567-003625); TSCD0044 (Elhady-FBITSC-PRIV003802-003806); TSCD0051 (Elhady-FBITSC-PRIV004326-004332); TSCD0067 (Elhady-FBITSC-PRIV004499-004521); TSCE0001 (Elhady-FBITSC-PRIV004627); TSCE0002 (Elhady-FBITSC-PRIV004628-4668); TSCE0003 (Elhady-FBITSC-PRIV004669-004678).

Plaintiffs' motion to compel: watchlisting policy exceptions; watchlisting training materials; selectee inclusion standards; differences between the 2013 and the 2015 Watchlisting Guidance; whether children can be included in the TSDB; whether friends, relatives, and associates of terrorists can be included in the TSDB; and whether non-investigative subjects can be included in the TSDB.

i. (U) Law Enforcement Interest in Nominations and Placement Documents Generally

22. (U) Specifically, disclosing the comprehensive policies and procedures concerning how placement in the TSDB, No Fly, and Selectee Lists occurs would reveal what type of conduct and other criteria would lead to an individual being placed in the TSDB. For example, the 2015 Watchlisting Guidance (TSCA0019), as well as various Nominations and Data Integrity Unit (NDIU) procedures and training materials,[2] contain detailed examples of various types of conduct that are taken into consideration to determine whether an individual meets the reasonable suspicion standard, as well as whether an individual is deemed operationally capable of engaging in or conducting a violent act of terrorism, one of the criteria for inclusion on the No Fly List.[3] This information would facilitate terrorists and terrorist groups in their operations and planning by assisting them in determining which individuals are likely already in the TSDB or those who are not. Such knowledge could also compromise ongoing counterterrorism investigations by giving members of terrorist groups the opportunity to gauge whether a

[2] (U) Training materials for TSC personnel necessarily include discussion of and methods for applying the law enforcement sensitive information contained in the WLG and standard operating procedures. Training materials requested by Plaintiffs include TSCA0004, TSCA0005, TSCA0006, TSCA0007, TSCA0013, TSCB0005, TSCB0006, TSCB0007, TSCB0009, TSCB0010, TSCB0012; TSCB0013, TSCB0016, TSCD0001, TSCD0008, TSCD0012, TSCD0013, TSCD0014, TSCD0016, TSCD0018, TSCD0022, TSCD0023, TSCD0024, TSCD0026, TSCD0027, and TSCD0029.

[3] (U) Examples of documents that describe specific inclusion criteria are TSCA0003, TSCA0004, TSCA0005, TSCA0006, TSCA0007, TSCA0008, TSCA0010, TSCA0011, TSCA0012, TSCA0013, TSCA0015, TSCB0012; TSCB0017-0037, TSCC0006, TSCD0006, TSCD0014, TSCD0023, TSCD0024, TSCD0029, TSCE0002, and TSCE0003.

particular individual is the subject of an FBI counterterrorism investigation, causing the person to alter his or her behavior, destroy evidence, take new precautions against surveillance, and change the level of any terrorism-related activity in which he or she is engaged. Disclosure of this information would also allow terrorists to discover the investigative procedures and techniques of investigating agencies and deduce those areas where investigative resources may not be focused. Terrorists would then be able to exploit the information to piece together how their activities may go undetected.

23. (U) Disclosure of the standards by which the TSC determines whether an individual should be added to or maintained on the Selectee List, either as a preliminary matter or as the result of redress, would enable terrorists and their associates to deduce which individuals are most likely to be subjected to enhanced security measures.[4] Such disclosure would allow terrorist groups to adjust assignments and recruiting efforts to focus on those persons who would be more likely to escape screening and security measures. This would provide members of those groups a greater chance of avoiding detection by law enforcement and intelligence officers while preparing terrorist operations. Finally, in some instances, disclosing the criteria for inclusion on the Selectee List might provide an individual who believes he is on the Selectee List enough additional information to deduce the nature or content of the underlying derogatory information the intelligence community has collected on him. This would allow the individual to identify the nature of investigative interest in him and to alter his behavior, destroy evidence, take new precautions against surveillance, and change the level of any terrorism-related activity in which he or she is engaged.24. (U) TSCD0013 is the final examination for the NDIU Basic Analyst

[4] (U) While the No Fly List criteria are set forth in the Overview of the U.S. Government's Watchlisting Process and Procedures at Elhady-FBITSC-001947-001956, the 2015 Watchlisting Guidance and other documents compelled by the plaintiffs contain a more detailed explanation and application of the No Fly List criteria with analysis of specific examples that have not been publicly disclosed.

Course and TSCD0014 is the answer key for the examination. Not only do these documents include law enforcement sensitive information about watchlisting policies and procedures, but releasing the examination and the answer key would also adversely affect TSC's ability to evaluate the knowledge and competency of its analysts. As a result, these documents must be protected as law enforcement sensitive.

24. (U) In sum, it is imperative that this category of documents regarding nominations and placement remain protected from disclosure since release of this information would reveal procedures and techniques for law enforcement investigations and intelligence gathering operations which could reasonably be expected to risk circumvention of the law and harm to national security.

25. (U//~~LES~~)

ii. (U) The 2015 Watchlisting Guidance and Associated Addendum

26. (U) While all the documents listed in this section warrant protection under the law enforcement privilege, the severe harm that would result from disclosure of the U.S. Government's 2015 Watchlisting Guidance ("Guidance"), logged as TSCA0019, and the associated addendum, logged as TSCD0004, warrants additional discussion.

27. (U) The Guidance is the U.S. Government's consolidated approach to terrorist identification, screening, and encounter management. Its drafting is coordinated by TSC and an interagency group under the auspices of the National Security Council and approved by the White House Deputies Committee (a group comprised of the deputy heads of agencies) and is the culmination of collaborative input from the intelligence community, law enforcement community, and homeland security elements. The Guidance is a compilation of unclassified, law enforcement sensitive information and Sensitive Security Information that, taken together, provides a comprehensive, particularized and granular compendium of the U.S. terrorism watchlisting enterprise, including its strategy, priorities, and processes. In essence, it is a comprehensive manual and a "roadmap" to one of the United States' critical national security programs in regard to protecting the homeland – terrorism watchlisting and screening. Accordingly, it is highly sensitive and the disclosure of it would cause significant harm to law enforcement and national security interests.

28. (U) The Guidance is disseminated solely within the U.S. Government watchlisting and screening communities and only to those who possess a need to know such information. Despite the extremely sensitive nature of the Guidance, it is marked unclassified in order to facilitate sharing with watchlisting and screening partners that have a need to know but would

not be able to access classified information.[5] Collectively, the information contained in the Guidance paints a detailed and comprehensive picture of the entire U.S. terrorism watchlisting enterprise, its strengths and weaknesses, capabilities, and limitations. It also describes how specific circumstances may or may not satisfy the applicable standards for terrorist watchlisting. Disclosure of the Guidance, a comprehensive watchlisting strategy, furnishes a platform for the analysis and design of measures to defeat or counteract the strategy. Moreover, while some individual pieces of this guidance may not seem harmful, disclosure of even these minor details may cause jeopardy to important federal interests because, much like a jigsaw puzzle, each detail may aid adversaries in piecing together information about the capabilities and limitations of the U.S. government's watchlisting and counterterrorism practices, and allow them to accumulate information about such practices in order to evade counterterrorism screening efforts.[6]

29. (U) The Guidance contains a significant amount of information relating to the following categories:

- Operational policies, procedures, and instructions for the units within the TSC that receive and process nominations, encounters, and redress referrals related to the TSDB or the No Fly and Selectee Lists;
- The specific criteria used to nominate a person to the TSDB or the No Fly and Selectee Lists, to include specific factual circumstances;
- FBI operational policies and procedures related to counterterrorism investigations and watchlisting;
- Terrorism watchlisting criteria, policies, and procedures from other federal

[5] (U) Treating highly-sensitive national security information as unclassified is particularly appropriate in the context of terrorist watchlisting, where certain extracts of classified information are "deemed unclassified" to facilitate sharing with watchlisting partners that would be unable to access classified information. Given the involvement of these partners in the watchlisting enterprise, it is equally necessary for them to be able to access the Watchlisting Guidance.

[6] (U) Indeed, while the 2015 Watchlisting Guidance was portion-marked with a view toward possibly releasing a redacted version to the public, it ultimately determined that releasing the Guidance, in any form, would present too great a threat to national security, providing adversaries valuable information about watchlisting standards and procedures and thereby enabling them to employ more effective counter-measures. Instead, the watchlisting community created the Overview Document, as the most comprehensive summary of the watchlisting enterprise that could be released without compromising national security.

government agencies; and

- Memoranda of understanding outlining the creation and implementation of the TSC and the TSDB.

30. (U) The Guidance also details several specific substantive topics which provide a roadmap of (among other things), the structure, nomination procedures, and identity elements of the U.S. terrorism watchlisting enterprise, the knowledge of which could be used to defeat the terrorism watchlisting process. Among these topics are:

- Watchlist nomination and removal procedures;
- Minimum substantive derogatory standards for terrorist watchlisting;
- Pre-conditions for placement on the No Fly or Selectee List;
- No Fly and Selectee List Criteria;
- Types of encounters with KSTs.

31. (U) The Guidance thus provides significant insight into the internal workings of the U.S. terrorism watchlisting process, including the type, quality, and amount of information needed to watchlist an individual, as well as how the information is vetted and disseminated throughout the intelligence community. The full extent of U.S. government policies and procedures concerning placement of individuals in the TSDB, or particular subsets of the TSDB, such as the Selectee List, have never been publicly revealed.[7] Disclosure of the Guidance would provide terrorists and their associates with a list of specific techniques and procedures by which the U.S. government gathers, evaluates, analyzes, identifies, and shares information concerning known or suspected terrorists (KSTs), and by which the U.S. government utilizes these various lists to protect the national security.

[7] (U) The FBI is aware that there is a document in the public domain that purports to be a leaked or stolen copy of the 2013 Watchlisting Guidance. The government has not confirmed or denied the authenticity of that document.

32. (U//~~LES~~) Specifically, disclosing the policies and procedures concerning how placement in the TSDB, No Fly, and Selectee Lists occurs would reveal what type of conduct and other criteria would lead to an individual being placed in the TSDB. For example, the Guidance contains detailed examples of various types of conduct that are taken into consideration to determine whether an individual meets the reasonable suspicion standard, as well as whether an individual is deemed operationally capable of engaging in or conducting a violent act of terrorism, one of the criteria for the No Fly List. This information would assist terrorists and terrorist groups in determining which individuals are likely already in the TSDB.

[redacted] Disclosure of this information would also allow terrorists to discover the investigative procedures and techniques of investigating agencies and deduce those areas where investigative resources may not be focused. Terrorists would then be able to exploit the information to piece together how their activities may go undetected.

33. (U//~~LES~~) The Guidance also extensively discusses U.S. government screening and encounter procedures. [redacted]

[redacted] This would adversely impact U.S. government's counterterrorism investigations and efforts.

34. (U//~~LES~~) [redacted]

35. (U) Finally, protecting the scope and extent of the watchlisting enterprise (as set forth in the Guidance) is crucial to sustaining the enterprise. Knowledge of the platforms, entities, and processes associated with terrorist screening, identification, and information collection could facilitate similar behavior designed to negate screening and identification. Ensuring ignorance of the extent of the enterprise, including unclassified details, is the first step in protecting it from exploitation by terrorists. Some information may prove dangerous when combined with other information by a knowledgeable actor (especially a hostile intelligence agency). Similarly, here, some isolated portions of the Guidance may not seem critical. However, considered as a whole, the Guidance is a comprehensive and detailed mosaic of the U.S. government consolidated strategy, procedure, and guidance for terrorist watchlisting. Disclosure of the Guidance would enable terrorist actors to deduce vulnerabilities in the watchlisting and screening enterprise and engineer effective countermeasures to facilitate undetected terrorist movement and activity. Such exposure would render the U.S. government watchlisting strategy – the first step in the U.S.

government's counterterrorism and national security strategy – far less effective, thus causing significant harm to law enforcement interests in counterterrorism investigations.[8]

36. (U//~~LES~~) Additionally, TSCD0004 is Addendum B to the MOU on the Integration and Use of Screening Information to Protect against Terrorism, which also is an attachment to the Watchlisting Guidance. This sensitive document provides information that reveals how the government accomplishes its terrorist screening and watchlisting mission. The document contains details about how different agencies process and coordinate information.

Such information presents a significant risk to national security by enabling adversaries to develop and employ more effective counter-measures to thwart terrorist screening efforts. Given this information, terrorists could change their pattern of life and their activities to thwart any further screening efforts and to further their terrorism goals. This could have the effect of impeding any further

[8] (U) The same would be true of any document that reflects portions of the Guidance or other sensitive internal TSC procedures, when considered together, and thus raise the same concerns. These documents would include TSCA0001, TSCA0002, TSCA0003, TSCA0004, TSCA0005, TSCA0006, TSCA0007, TSCA0008, TSCA0009, TSCA0010, TSCA0011, TSCA0012, TSCA0013, TSCA0017, TSCA0018, TSCB0004, TSCB0006, TSCB0010, TSCB0012, TSCB0013, TSCB0014, TSCB0016, TSCC0006, TSCD0002, TSCD0003, TSCD0004, TSCD0006, TSCD0008, TSCD0009, TSCD0014, TSCD0015, TSCD0023, TSCD0024, TSCD0026, TSCD0029, TSCD0046, TSCD0049, TSCD0053, TSCD0065, TSCE0001, TSCE0002, and TSCE0003.

counterterrorism efforts by the FBI or its law enforcement partners since the known behavior of the associates would change, causing the FBI to lose valuable intelligence about their activities.

37. (U//~~LES~~) [redacted]

38. (U//~~LES~~) Many of these documents also discuss sensitive law enforcement techniques, [redacted]

B. (U) Information Sharing

39. (U) Agencies and officials authorized or required to conduct terrorist screening or to use information for diplomatic, military, intelligence, law enforcement, immigration, transportation security, visa, and protective processes are given access to terrorism information to facilitate their respective public missions. Information from the TSDB is shared with domestic and foreign government entities for national security purposes and is not generally available to the public or private entities without a government function. Documents relating to information sharing sought by Plaintiffs include, without limitation, documents listed in

Plaintiffs' Exhibit K[9] and the following specific information sought by Plaintiffs' motion to compel: whether courts have access to TSDB information; information sharing for Secure Flight, immigration, and visas; ability of downstream agencies and foreign partners to disseminate TSDB data; and actual access to TSDB information by partners and downstream sharing.

40. (U) Some of the information sharing documents requested by plaintiffs include specific details regarding the information technology infrastructure and security of TSC and partner systems (e.g., TSCD0052, TSCC0004, TSCC0005, TSCD0029, TSCD0049, and TSCD0059). Such information could be valuable to adversaries of the United States in their efforts to access, alter, or otherwise disrupt terrorist screening systems. For example, a document identifying specific firewalls that protect data at the TSC and in partner systems would

[9] (U) TSCA0017; TSCA0018; TSCA0030-0225; TSCA0229; TSCA0230; TSCA0231; TSCA0233; TSCA0235; TSCB0002 (Elhady-FBITSC-PRIV00002); TSCB0009 (Elhady-FBITSC-PRIV00273-00298); TSCB0010 (Elhady-FBITSC-PRIV00299-00319); TSCB0012 (Elhady-FBITSC-PRIV00320-00346); TSCC0003 (Elhady-FBITSC-PRIV002704-002719); TSCC0004 (Elhady-FBITSC-PRIV002720-002758); TSCC0005 (Elhady-FBITSC-PRIV002759-002842); TSCC0006 (Elhady-FBITSC-PRIV002843-002851); TSCC0007 (Elhady-FBITSC-PRIV002852-002855); TSCC0008 (Elhady-FBITSC-PRIV002856-002858); TSCC0009 (Elhady-FBITSC-PRIV002859-002866); TSCC0010 (Elhady-FBITSC-PRIV002867-002989); TSCC0011 (Elhady-FBITSC-PRIV002990-003098); TSCD0001 (Elhady-FBITSC-PRIV003099-003104); TSCD0002 (Elhady-FBITSC-PRIV003105-003117); TSCD0003 (Elhady-FBITSC-PRIV003118-003129); TSCD0004 (Elhady-FBITSC-PRIV003130-003140); TSCD0008 (Elhady-FBITSC-PRIV003150-003184); TSCD0017 (Elhady-FBITSC-PRIV003291-003293); TSCD0032 (Elhady-FBITSC-PRIV003670-003671); TSCD0033 (Elhady-FBITSC-PRIV003672-003673); TSCD0034 (Elhady-FBITSC-PRIV003674-003682); TSCD0036 (Elhady-FBITSC-PRIV003690-003691); TSCD0037 (Elhady-FBITSC-PRIV003692-003699); TSCD0039 (Elhady-FBITSC-PRIV003702-003714); TSCD0040 (Elhady-FBITSC-PRIV003715-003719); TSCD0042 (Elhady-FBITSC-PRIV003724-003726); TSCD0045 (Elhady-FBITSC-PRIV003807-003816); TSCD0046 (Elhady-FBITSC-PRIV003817-003827); TSCD0047 (Elhady-FBITSC-PRIV003828-003839); TSCD0048 (Elhady-FBITSC-PRIV003840-003851); TSCD0049 (Elhady-FBITSC-PRIV003852-004243); TSCD0050 (Elhady-FBITSC-PRIV004244-004325); TSCD0052 (Elhady-FBITSC-PRIV003333-003342); TSCD0053 (Elhady-FBITSC-PRIV004343-004357); TSCD0054 (Elhady-FBITSC-PRIV004358-004371); TSCD0055 (Elhady-FBITSC-PRIV004372-004377); TSCD0056 (Elhady-FBITSC-PRIV004378-004383); TSCD0057 (Elhady-FBITSC-PRIV004384-004399); TSCD0058 (Elhady-FBITSC-PRIV004400-004404); TSCD0059 (Elhady-FBITSC-PRIV004405-004412); TSCD0060 (Elhady-FBITSC-PRIV004413-004418); TSCD0061 (Elhady-FBITSC-PRIV004419-004424); TSCD0062 (Elhady-FBITSC-PRIV004425-004426); TSCD0063 (Elhady-FBITSC-PRIV004427-004443); TSCD0064 (Elhady-FBITSC-PRIV004444-004445); TSCD0065 (Elhady-FBITSC-PRIV004446-004448); TSCD0066 (Elhady-FBITSC-PRIV004489-004498); TSCD0067 (Elhady-FBITSC-PRIV004499-004521); TSCD0070 (Elhady-FBITSC-PRIV004548-004561); TSCD0071 (Elhady-FBITSC-PRIV004562-004626).

let an adversary know exactly what firewalls it would need to bypass in order to access this information.

41. (U//~~LES~~) Similarly, some of the information sharing documents requested by plaintiffs provide details regarding the specific identifying information TSC exports to its domestic and foreign partners (e.g., foreign partner arrangements, TSCA0003, TSCC003-005, and TSCD0029). Knowledge of such information would enable terrorists to alter the tactics and behaviors to avoid detection by means of the specific information individual agencies use in terrorist screening.

42. (U//~~LES~~) Additionally, some of the documents requested by plaintiffs include descriptions of law enforcement handling codes, This would divulge specific law enforcement methods and should be protected as law enforcement sensitive.

i. (U) Domestic Partners

43. (U) Documents relating to information sharing with domestic partners (e.g., TSCC0003, TSCC0004, TSCC0005, TSCC0007, TSCC0008, TSCC0009, TSCD0002, TSCD0032, TSCD0033, TSCD0034, TSCD0036, TSCD0037, TSCD0039, TSCD0040, TSCD0042, TSCD0045, TSCD0046, TSCD0047, TSCD0048, TSCD0049, TSCD0055,

TSCD0056, TSCD0057, TSCD0058, TSCD0059, TSCD0060, TSCD0061, TSCD0062, TSCD0063, TSCD0064, and TSCD0070) would reveal details of the United States' comprehensive, multi-agency approach to combating terrorism. If terrorists and their associates learn the comprehensive details of what information individual agencies use in their screening activities, along with detailed specifics regarding how they use that information, such terrorists would be able to tailor their strategies and methods to avoid detection by U.S. law enforcement and screening authorities and maximize their destructive impact. Disclosure of this information would cause irreparable damage to investigations pertaining to terrorism, and undermine the years of hard work and collaboration the U.S. government agencies have devoted to protecting the homeland from terrorism since 9/11.

44. (U) In recent years, through the information sharing system supported by the TSDB, the United States has been able to track potential terrorist plots by coordinating derogatory information from the intelligence community with encounter information from local law enforcement or other screening partners.

45. (U//~~LES~~) [redacted] As was noted by the 9-11 Commission, this was not possible before 9-11 when, for example, the CIA might have known an individual had ties to terrorism--but did not know the individual was in the United States, while local law enforcement knew the individual was in the United States--but did not know the individual had ties to terrorism. The common operating picture afforded by the information sharing system (as supported by the TSDB) is absolutely critical to preventing such terrorist plots from coming to fruition in the future.

ii. (U) Foreign Partners

46. (U) The TSC has a mandate, pursuant to Homeland Security Presidential Directive-6 (HSPD-6), to exchange terrorism screening information with select foreign partners. Through a series of international arrangements, memoranda of understanding, mutual legal assistance treaties, letters rogatory, other voluntary and compulsory agreements, and professional relationships between the United States and foreign governments, the United States shares and receives information for the purpose of combating terrorism. The FBI's ability to carry out its responsibilities to conduct counterterrorism investigations and to collect foreign intelligence often depends on the cooperation of foreign government officials, foreign intelligence services, or foreign security services.

47. (U//~~LES~~) Documents TSCA0030-0225 evidence terrorism screening information sharing arrangements between the United States and its foreign partners (foreign partner arrangements). These foreign partner arrangements identify what information participants agree to share, how participants share that information, and the specific points of contact that coordinate the information sharing. While four of these foreign partner arrangements exist in the form of binding international agreements, which are necessarily public,[10] the vast majority of such foreign partner arrangements are embodied in non-public documents meant to be protected against disclosure. In fact, some of the documents evidencing foreign partner arrangements are specifically classified, in whole or in part, and are the subject of an assertion of the State Secrets Privilege. Even when not specifically classified, however, foreign partner arrangements are

[10] (U) The binding international agreements between the United States and Albania, Bulgaria, Hungary, and Slovenia are publicly available on the Department of State Treaty Office website. While these agreements were inadvertently included amongst the foreign partner documents listed on the privilege log, the United States is not seeking to protect these documents as law enforcement sensitive and has already provided them to plaintiffs via interrogatory response. Any reference in this section to "foreign partner arrangements" is not meant to include these four binding international agreements.

sensitive and exist pursuant to an understanding that their terms (and often their existence) will be protected against disclosure.[11] Consequently, TSC neither confirms nor denies the existence of foreign partner arrangements with many foreign partners.[12] Moreover, because the contents of foreign partner agreements would disclose law enforcement sensitive information in the context of combating terrorism outside the United States, the TSC protects foreign partner agreements against unauthorized disclosure.

48. (U) The purpose of a foreign partner arrangement is to provide the United States and its foreign partner (which may be a foreign government or a military, intelligence, or law enforcement component of the foreign government) a mechanism to collaborate and coordinate on national security threats through the exchange of identifiers associated with KSTs. Incorporated within these distinct arrangements are law enforcement-privileged matters related to procedures for sharing information and encounter management.[13] Such information could reasonably be expected to enable US adversaries to employ more effective countermeasures or even to disrupt terrorist screening systems.

49. (U) Additionally, a failure by the United States to honor the expectation of these foreign partners that their information will be protected against unauthorized disclosure could reasonably be expected to affect the trust these countries have in the United States and their willingness to share sensitive information, which is critical to the United States' global effort to

---

[11] (U//~~LES~~) While the United States has generally acknowledged the existence of such arrangements with all Visa Waiver Program (VWP) countries, the actual arrangements with each of these countries remain sensitive. [redacted] This evidences the fact that acknowledging the existence of an arrangement is not the same as disclosing the terms of such an arrangement.

[12] (U) This remains true regardless of any disclosure made by foreign partners because, if TSC were to disclose information without specific authorization from the partner, this could undermine the trust of other foreign partners that rely on the TSC's assurances of nondisclosure or confidentiality.

[13] (U) An "encounter" is generally defined as any instance where a federal, state, local, tribal, territorial, or international partner comes in contact with a KST, such as through a traffic stop or a border crossing.

combat terrorism. For example, disclosure of the United States' arrangement with any particular foreign partner might create diplomatic problems between that foreign partner and other countries less friendly to the United States. This, in turn, might reasonably be expected to adversely affect the foreign partner's willingness to cooperate with the United States in the future. Moreover, certain countries might not cooperate with the United States if they knew other countries they consider adversaries were also cooperating with the United States. Less cooperation from these foreign partners would increase the risk for potential terrorist incidents because the United States would be less informed about potential threats. As a result, a strict uniform policy of not disclosing foreign partner arrangement ensures maximal informational advantage for the United States which results in an increased capability of preventing and deterring terrorist attacks.

50. (U) Additionally, the information sharing arrangements with foreign partners and other documents pertaining to these arrangements (e.g., TSCA0235, TSCA0229, TSCB0009, TSCD0008, TSCD0017, and TSCD0029) provide specific processes for the use and dissemination of the shared terrorism screening information. If terrorists and their associates learn the names of all countries with which the U.S. government exchanges terrorism information and the details of those arrangements, they reasonably could alter their behavior or strategies overseas, including shifting their activities away from countries with which the United States has information sharing arrangements, to those countries with which the United States does not have such arrangements. Additionally, because of the expected confidentiality of these foreign partner arrangements, the disclosure of this information would undermine the United States' foreign partner relationships, jeopardize ongoing collaborative efforts, and chill future cooperation of TSC's foreign partners. To publicly disclose the existence of terrorism screening

arrangements when a foreign partner has asked for confidentiality would cause others not to trust the United States' representations regarding protecting the existence of arrangements or any information in those arrangements. Given the existence of terrorists and their associates in foreign countries and the ease with which they travel overseas, the ability to protect this information and maintain trust with foreign partners is critical to the U.S. government's watchlisting and screening efforts as well as the international effort to address the threat of international terrorism. Thus, information pertaining to foreign partners should continue to be protected, as its release could reasonably be expected to harm counterterrorism investigations and efforts.

51. (U) Even if the names of foreign partners are redacted from the foreign partner documents, the documents themselves may provide clues that would allow a reader to identify the countries to which they pertain. For example, some foreign partner documents are written in languages other than English and use dialects that might allow U.S. adversaries to identify the countries to which they pertain. Other foreign partner documents include specific provisions to address specific laws, policies, or concerns and specific word choices to address translation issues, local usage, etc. Each of these factors might allow adversaries to identify countries with which the United States has information sharing arrangements.

52. (U) To the extent Plaintiffs only seek to discover provisions pertaining to further dissemination of TSDB information by foreign partners, all agreements/arrangements for the sharing of TSDB information with foreign partners include representations to the effect that the foreign partner will use TSDB information only for terrorist screening, will safeguard TSDB information from unauthorized disclosure, and will not, without express permission, disclose TSDB information publicly or to any private entity, private individual, other government, or

international organization. It is therefore unnecessary for plaintiffs to examine individual foreign partner documents for this purpose. Moreover, plaintiffs already have representative samples of such provisions in the Albanian, Bulgarian, Hungarian, and Slovenian agreements they have already been provided.

53. (U) Several of the documents within TSCA0030-0225 describe the technical intricacies of how information will be exchanged between the United States and a particular foreign partner or are transmittal, coordination, or modification documents. Such documents do not pertain to further dissemination or restrictions thereon, with those obligations and restrictions being contained in other documents, such as memoranda of understanding. Since these documents do not pertain to "further dissemination," they are outside the scope of documents Plaintiffs seek to compel in their motion. Such documents would include TSCA0034, TSCA0056, TSCA0058, TSCA0065, TSCA0072, TSCA0079, TSCA0085, TSCA0094, TSCA0104, TSCA0105, TSCA0109, TSCA0119, TSCA0171 and TSCA0185.

54. (U) Finally, several of the documents within TSCA0030-0225 are foreign language translations of English documents within TSCA0030-0225 and would provide Plaintiffs a mechanism to identify the specific foreign partner to which a particular document relates, even were the name of that foreign partner to be withheld. These documents include TSCA0049, TSCA0059, TSCA0061, TSCA0068, TSCA0087, TSCA0104, TSCA0124, TSCA0137, TSCA0146, TSCA0164, TSCA0169, TSCA0174, TSCA0187, TSCA0189, TSCA0191, TSCA0192, TSCA0196, TSCA0198, TSCA0200, TSCA0203, TSCA0205, TSCA0207, TSCA0209, TSCA0211, TSCA0214, TSCA0216, TSCA0218, and TSCA0220.

iii. (U) TSC Contracts

55. (U) In their motion, Plaintiffs also request production of the government's contracts with certain companies that provide much of the work force at TSC (Strategic Operation Solutions and Sotera). Plaintiffs' alleged purpose for requesting these documents relates to "their access to and dissemination of TSDB information." Prior to having access to TSDB information, all TSC contractors are required to sign security and non-disclosure agreements that prohibit unauthorized dissemination of TSDB information. Disclosure of additional details regarding the services provided by these companies and their employees might allow US adversaries to target them for exploitation and would therefore pose a threat to national security. Additionally, the Government is prohibited from disclosing certain proprietary and business confidential information about the companies' contracts with the Government.

C. (U) Screening and Encounters

56. (U) The policies and procedures Plaintiffs seek in their motion to compel also reflect U.S. Government screening and encounter strategies. These documents include, without limitation, documents listed in Plaintiffs' Exhibit K.[14]

57. (U) Documents pertaining to TSC's internal procedures for tracking encounters with individuals listed in the TSDB (e.g., TSCA0017, TSCA0018, and TSCD0029) do not have any effect that would be noticeable to the listed individual. For example, the fact that TSC may record that a particular individual has booked a flight does not affect whether the individual will be able to board the flight or subject to enhanced security screening. Similarly, the fact that TSC

[14] (U) TSCA0017; TSCA0018; TSCA0230; TSCA0231; TSCA0233; TSCB0010 (Elhady-FBITSC-PRIV00299-00319); TSCC0011 (Elhandy-FBITSC-PRIV002990-03098);TSCB0012 (Elhady-FBITSC-PRIV000320-000346); TSCD0029 (Elhady-FBITSC-PRIV003567-003625); TSCD0050 (Elhady-FBITSC-PRIV004244-004325); TSCD0054 (Elhady-FBITSC-PRIV004358-004371); TSCD0055 (Elhady-FBITSC-PRIV004372-004377); TSCD0064 (Elhady-FBITSC-PRIV004444-004445); TSCD0065 (Elhady-FBITSC-PRIV004446-004488); TSCD0066 (Elhady-FBITSC-PRIV004489-004498); TSCD0067 (Elhady-FBITSC-PRIV004499-004521); TSCD0071 (Elhady-FBITSC-PRIV004562-004626).

may record an encounter between a listed individual and a local police officer will not affect whether the officer issues the individual a citation, arrests the individual, etc. Nonetheless, details contained in these documents could, if released publicly, lead to counter measures by terrorists and their associates that would compromise screening, watchlisting, and counterterrorism efforts.

58. (U) Similarly, documents pertaining to the screening measures employed by TSC's domestic partners (e.g., TSCA0003, TSCC0003, TSCC0004, TSCC0005, TSCC0007, TSCC0008, TSCC0009, TSCD0002, TSCD0032, TSCD0033, TSCD0034, TSCD0036, TSCD0037, TSDC0039, TSCD0040, TSCD0042, TSCD0045, TSCD0046, TSCD0047, TSCD0048, TSCD0049, TSCD0055, TSCD0056, TSCD0057, TSCD0058, TSCD0059, TSCD0060, TSCD0061, TSCD0062, TSCD0063, TSCD0064, TSCD0066, TSCD0070, and TSCD0071) would, if released publicly, allow US adversaries to develop and employ countermeasures at the point of screening. Again, this would significantly compromise, screening, watchlisting, and counterterrorism efforts.

59. (U//~~LES/SSI~~) [redacted]

[redacted]

[redacted]

60. (U) TSCD0065 (An Updated Strategy for Comprehensive Terrorist-Related Screening Procedures) provides a detailed and comprehensive description of the US terrorist screening enterprise. Like the Guidance, disclosure of this information would provide a roadmap to US adversaries, allowing them to better evade and circumvent terrorist screening systems and could reasonably be expected to cause significant harm to national security.

D. (U) Redress Policy Documents

61. (U) The "Redress Policy Documents" requested by Plaintiffs (TSCA0014 and TSCD0051) contain law enforcement sensitive information pertaining to specific sources and methods employed by redress personnel, coordination with other members of the intelligence community, and sensitive internal procedures.

62. (U//~~LES~~) [redacted]

[redacted]

E. (U) Identities and Contact Information

63. (U) Certain documents sought by Plaintiffs include, among other things, the names of TSC and FBI personnel working on sensitive law enforcement and counterterrorism matters or specific contact information for government personnel or units. This information is scattered throughout many of the documents listed in Exhibit K.[15] Law enforcement personnel routinely

[15] (U) These document include, without limitation, TSCA0015; TSCA0233; TSCB0005 (Elhady-FBITSC-PRIV000019-000070); TSCB0010 (Elhady-FBITSC-PRIV000299-000319); TSCB0016 (Elhady-FBITSC-

face threats to their security, and these safety and security concerns are heightened when, as here, the government personnel in question have worked or are working on counterterrorism cases. Given that their work involves detecting and thwarting the efforts of terrorists and their associates, these government personnel, as well as their family members, can be targeted by terrorists or their sympathizers and are particularly vulnerable to threats, retaliation, and physical harm. Disclosure of the information sought by Plaintiffs thus puts TSC and FBI personnel at personal risk, with resulting harm to the affected individuals and the FBI's investigative and law enforcement efforts. This information is routinely guarded for purposes of safety and security.

64. (U//~~LES~~) [redacted]

[redacted]

F. (U) **Audit Documents**

65. (U) Plaintiffs in this action also seek to compel privileged portions of two audit documents: TSCC0010, an October 2007 Government Accountability Office ("GAO") Report entitled "Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List

---

PRIV000396-000423); TSCC0003 (Elhady-FBITSC-PRIV002704-002719); TSCC006 (Elhady-FBITSC-PRIV002843-002851); TSCC0008 (Elhady-FBITSC-PRIV002856-002858); TSCC0009 (Elhady-FBITSC-PRIV002859-002866); TSCC0010 (Elhady-FBITSC-PRIV002867-002989); TSCC0011 (Elhady-FBITSC-PRIV002990-003098); TSCD0001 (Elhady-FBITSC-PRIV003099-003104); TSCD0002 (Elhady-FBITSC-PRIV003105-003117); TSCD0006 (Elhady-FBITSC-PRIV003144); TSCD0023 (Elhady-FBITSC-PRIV003488-003515); TSCD0032 (Elhady-FBITSC-PRIV003670-003671); TSCD0033 (Elhady-FBITSC-PRIV003672-003673); TSCD0034 (Elhady-FBITSC-PRIV003674-003682); TSCD0037 (Elhady-FBITSC-PRIV003692-003699); TSCD0039 (Elhady-FBITSC-PRIV003702-003714); TSCD0045 (Elhady-FBITSC-PRIV003807-003816); TSCD0047 (Elhady-FBITSC-PRIV003828-003839); TSCD0048 (Elhady-FBITSC-PRIV003840-003851); TSCD0049 (Elhady-FBITSC-PRIV003852-004243); TSCD0057 (Elhady-FBITSC-PRIV004384-004399); TSCD0061 (Elhady-FBITSC-PRIV004419-004424); TSCD0062 (Elhady-FBITSC-PRIV004425-004426); TSCD0067 (Elhady-FBITSC-PRIV004499-004521)); TSCD0070 (Elhady-FBITSC-PRIV004548-004561), as well as documents included in TSC0030-0225 (foreign partner arrangements).

("GAO Report"), and TSCC0011, a March 2014 audit prepared by DOJ's Office of the Inspector General ("OIG"), entitled "Audit of the Federal Bureau of Investigation's Management of Terrorist Watchlist Nominations" ("OIG Report"). Redacted versions of both documents are publically available.[16]

66. (U) The public version of the GAO Report omits certain information associated with vulnerabilities that the GAO identified in then-extant screening processes and measures that the GAO noted could be taken to address those vulnerabilities. It also omits certain details regarding (1) certain policies and procedures associated with the development and use of the TSDB, (2) specific outcomes of encounters with individuals who were positively matched to the TSDB; and (3) certain statistical information relevant to the watchlisting enterprise.

67. (U//~~LES~~) [redacted] Further, the disclosure of the various statistics that have been omitted from the public version of the GAO Report would be harmful for the reasons discussed in Subsection G, below.

68. (U) The public version of the OIG Report redacts certain information that is, inter alia, either classified and/or protected by the law enforcement privilege. I understand that in

[16] (U) Defendants produced the public version of the GAO Report to Plaintiffs at Elhady-FBITSC000680-000763. The public version of the OIG report is available at: https://oig.justice.gov/reports/2014/a1416.pdf. Plaintiffs additionally include TSCD0067, the Privacy Impact Assessment for the Terrorist Screening Database – Terrorist Screening Database (the "PIA") under the heading of "audit" documents which they seek to compel Defendants to produce. The PIA is not properly categorized as an audit document, but it does describe and discuss the watchlisting enterprise in specific detail, and is properly withheld under the rationales stated in Subsections A, B, C, and G of this declaration, including but not limited to the comprehensive insight it would provide into the functioning of the United States' watchlisting system

their motion to compel, Plaintiffs stated that with respect to the OIG Report, they do not seek the production of any information that remains classified, but requested that Defendants determine whether any previously classified information "may now be disclosed." Accordingly, the portions of the OIG Report that are presently marked as classified is being referred to an appropriate Original Classification Authority ("OCA") for a review to determine whether the information in question remains classified. While that review is not yet complete as of the signing of this declaration, I expect that such review will be completed in the near future.

69. (U//~~LES~~) In addition to and separate from the classification redactions to the publically available OIG Report, certain information in that document is redacted because it is protected by the law enforcement privilege. [redacted] The disclosure of this information would risk harming national security and facilitating the circumvention of counter-terrorism efforts [redacted]

[redacted]

G. (U) TSDB Statistics

70. (U) Plaintiffs in this case have requested certain TSDB statistics,[17] including the Director's Monthly Reports, Weekly Statistical Reports, Monthly Statistical Reports, Error reports, effectiveness reports or audits, and cost-benefit analyses. Additionally, plaintiffs have specifically requested the total number of nominations by the FBI to the watchlist and the number of those nominations that were rejected, the yearly average number of persons nominated to the No Fly list and the number of those nominations TSC accepted, the total number of individuals on the No Fly list for each year from 2012 until present, the total number of times individuals on the No Fly list have been permitted to fly, the yearly average number of persons nominated to the Selectee list as well as how many of those nominations were accepted, the total number of individuals on the Selectee list from 2012 to present, the total number of U.S. citizens on the Selectee list for each year from 2012 until present, the total number of individuals currently in the TSDB that have not been charged or convicted of a terrorism-related offense, the total number of individuals nominated or accepted for inclusion in the TSDB with the words "Islam" or "Muslim" contained in the nomination, the yearly average number of encounters with

[17] (U) Documents containing TSDB statistical information include, without limitation, TSCA0229; TSCB0009 (Elhady-FBITSC-PRIV000273-000298); TSCB0016 (Elhady-FBITSC-PRIV000396-000423); TSCC0001 (Elhady-FBITSC-PRIV000445-001912); TSCC0002 (Elhady-FBITSC-PRIV001913-002703); TSCC0004 (Elhady-FBITSC-PRIV002720-002758); TSCC0005 (Elhady-FBITSC-PRIV002759-002842); TSCC0010 (Elhady-FBITSC-PRIV002867-002989); TSCC0011 (Elhady-FBITSC-PRIV002990-003098); TSCC0043 (Elhady-FBITSC-PRIV003727-003801); TSCD0008 (Elhady-FBITSC-PRIV003150-003184); TSCD0016 (Elhady-FBITSC-PRIV003269-003290); TSCD0017 (Elhady-FBITSC-PRIV003291-003293); TSCD0018 (Elhady-FBITSC-PRIV003294-003303); TSCD0026 (Elhady-FBITSC-PRIV003520-003535); TSCD0027 (Elhady-FBITSC-PRIV003536-003546); TSCD0046 (Elhady-FBITSC-PRIV003817-003827); TSCD0049 (Elhady-FBITSC-PRIV003852-004243); TSCD0052 (Elhady-FBITSC-PRIV004333-004342); TSCD0054 (Elhady-FBITSC-PRIV004358-004371); TSCD0058 (Elhady-FBITSC-PRIV004400-004404); TSCD0059 (Elhady-FBITSC-PRIV004405-004421); TSCD0067 (Elhady-FBITSC-PRIV004499-004521).

individuals placed on the watch list that were recorded by TSC, the number of terrorist attacks committed within the United States within the last decade, the number of perpetrators of terrorist attacks within the United States within the last decade, the number of perpetrators of terrorist attacks within the United States within the last decade who were listed in the TSDB, and the aggregate number of children under age 10 or under age 5 included in the TSDB.

71. (U) As a preliminary matter, it is not clear precisely what information these interrogatories are seeking. Moreover, the TSC does not track much of the information requested by plaintiffs. And, while it may be possible for TSC to collect some of this information, doing so would essentially require a record-by-record analysis and comparison to information in the possession of other agencies. Such an endeavor would not only be unduly burdensome; it would harm national security by diverting resources from TSC's round-the-clock responsibilities of processing nominations, sharing information, and resolving encounters. The same would be true of plaintiffs' request for terrorist attacks within the United States.[18]

72. (U) For example, since there is no specific field in the TSDB to indicate whether an individual has been charged with or convicted of a terrorism-related offense, an analyst would essentially have to compare each record in the TSDB to the underlying derogatory information (which is not included in the TSDB) in the hope of finding some information regarding the

[18] (U) The FBI is, of course, aware of successful terrorist attacks in the United States, as is the general public. But plaintiffs' actual interrogatory was worded much differently. Terrorism has several different legal definitions, depending on context, and the interrogatory could seek information about acts of domestic terrorism or international terrorism, acts of terrorism as punishable under various federal or state laws in the United States or under the laws of another country, or it could include related criminal or noncriminal activity directly or indirectly related to such acts or attempts, or it could include nonpublic information about suspected terrorist activity, regardless of whether such activity culminated in violent attacks inside the United States. The request is also vague in that it seeks a response as to what the FBI "considers" criminal and terrorist acts. It also fails to define "acts . . . occurring within the United States;" the location of an act could be based solely upon where the harm occurred, or it could be based upon where harm was intended to occur, where one or more the conspirators or accomplices were located, where instrumentalities of the crime were located, or where necessary actions or processes forming part of the act or offense took place. FBI does not compile any of these specific categories of data and attempting to compile them would be unduly burdensome and certainly disproportionate to the needs of the case.

subject's arrest or conviction status, should any such information exist. Such a process would be extremely labor-intensive and time-consuming, and divert valuable resources away from TSC's critical mission to evaluate nominations to the TSDB and manage potential matches to the TSDB.

73. (U) Moreover, while some of the statistics requested by plaintiffs may seem harmless (such as the number of nominations or encounters received by TSC during a particular period), detailed statistics related to nominations and encounters can themselves reveal information that would be valuable to terrorists.

74. (U//~~LES~~)

75. (U//~~LES~~)

76. (U//~~LES~~) Additionally, information regarding the number of people meeting specific criteria in any given category (e.g., U.S. citizens or children) that are included in the TSDB, the No Fly list, or the Selectee list could be invaluable to terrorists in selecting operatives that are more likely to avoid detection because they are less likely to be identified during screening.

[redacted] It is not beyond the realm of possibility that a terrorist might exploit such information to the detriment of national security. [redacted]

77. (U//~~LES~~) The monthly TSC Dashboard reports (TSCD0043) provide precise numbers for nominations and encounters, on a monthly basis. As described above, knowledge of these changing statistics would allow sophisticated adversaries to draw conclusions regarding sensitive government policies and the focus of law enforcement and intelligence community efforts to combat terrorism. This is even more true of the weekly statistical reports (TSCC0002), which provide such specific statistical changes, along with trend analysis, for even smaller periods of time, and the TSC Monthly Director's Reports which provide granular information, on a monthly basis. [redacted]

[19] (U) To be placed in the TSDB as a KST, No Fly, or Selectee, a minor would have to meet all applicable standards and criteria. The minor's age would be one factor that would be considered.

[redacted] This level of insight into US policies and operations would provide a tremendous strategic advantage to US adversaries and could reasonably be expected to cause significant harm to national security.

H. (U) TSDB Status

78. (U) While Plaintiffs' motion to compel does not specifically seek the watchlist status of Plaintiffs or other specific individuals, it is important to emphasize why disclosure of such information would endanger national security and undermine Government efforts to combat terrorism.

79. (U//~~LES~~) TSDB information comes from sensitive law enforcement and counterterrorism investigations and classified sources and methods. [redacted]

[redacted]

80. (U//~~LES/SSI~~) [redacted]

[redacted] On the other hand, an individual who is not in the TSDB may be subject to additional inspection or screening, [redacted], for a wide variety of reasons unrelated to the terrorist watchlist. Thus, it cannot be argued that a known or suspected terrorist will necessarily be able to deduce his or her own status in the TSDB based upon his experiences at airports or at the border.

81. (U) Moreover, if the government were to disclose an individual's lack of status in the TSDB (i.e., that the individual is *not* in the TSDB), this would necessarily confirm that any

individual not eligible for such a disclosure *is*, in fact, in the TSDB. It would also be of considerable value to terrorist groups to confirm which individuals are not the subject of ongoing investigations and who are thus more likely to escape scrutiny. In other words, efforts to reverse engineer information based on what is confirmed would be significantly simplified for those seeking to do harm.

82. (U//~~LES~~) In addition, access to this information would allow terrorists to discover the investigative procedures and techniques of investigating agencies associated with an individual's status and, as a result, identify those areas where investigative resources may not be focused.

[redacted]

Disclosure of this information could thus reasonably be expected to risk circumvention of the law and cause harm to national security.

83. (U) Even where an individual has been denied boarding or has been subject to enhanced screening, the lack of official confirmation of TSDB status is still valuable to the Government in its watchlisting and screening efforts. Because there are many reasons an individual might be denied boarding or subject to enhanced screening that have nothing to do with TSDB status, the ambiguity left open by the absence of official confirmation operates to the Government's advantage in this context.

III. (U) ADDITIONAL HARM OF CUMULATIVE DISCLOSURES

84. (U) Protecting the scope and extent of the watchlisting enterprise (as set forth in the Law Enforcement Sensitive documents Plaintiffs seek to compel) is crucial to sustaining the watchlisting enterprise. Knowledge of the platforms, entities, and processes associated with terrorist nominations, information sharing, screening, identification, and information collection

could facilitate behavior designed to negate screening and identification. Protecting the extent of the enterprise, including unclassified details, from disclosure is the first step in protecting it from exploitation by terrorists. Even details that may seem innocuous in isolation could, when considered as a whole by a knowledgeable actor (especially a sophisticated terrorist organization), provide a comprehensive and detailed mosaic of the United States Government's consolidated watchlisting strategy. In other words, like a jigsaw puzzle, each detail about the watchlisting enterprise may aid adversaries in piecing together information about the United States' overall capabilities and limitations. Thus, disclosure of this law enforcement sensitive information would enable terrorist actors to deduce vulnerabilities in the watchlisting and screening enterprise and engineer effective countermeasures to facilitate undetected terrorist movement and activity. Such exposure would render the United States' watchlisting strategy far less effective, thus causing harm to law enforcement and national security interests.

85. (U) An excellent example of this risk is represented by the 2015 Watchlisting Guidance and the careful efforts that have been made to protect that document in its entirety. As described in Footnote 6, while the 2015 Watchlisting Guidance was portion-marked with a view toward possibly releasing a redacted version to the public, it ultimately determined that releasing the Guidance, in any form, would allow adversaries to piece together a complete picture of the United States' watchlisting enterprise. This presented too great a threat to national security, as it would provide adversaries valuable information about watchlisting standards and procedures and thereby enable them to employ more effective counter-measures. Instead, the watchlisting community created the Overview Document described in Paragraph 16, as the most comprehensive summary of the watchlisting enterprise that could be released without compromising national security.

IV. (U) PROTECTIVE ORDER

86. (U) Given the sensitivities of the information and the national security and law enforcement harms at stake, release of information in any form, even under a protective order, poses far too great a risk to national security. In the event the Court chooses to release information subject to a protective order, the release should be for attorney's eyes only and limited to discrete, necessary pieces of information that are directly relevant to Plaintiffs' claims.

V. (U) SENSITIVE SECURITY INFORMATION

87. (U) It is my understanding that TSA has the authority to designate certain information and categories of information as Sensitive Security Information. See 49 U.S.C. § 114(r)(1)(C), 49 C.F.R. §§ 1520.5(a), 1520.9(a)(1). The TSC referred to TSA certain documents deemed relevant for SSI review.

(U) CONCLUSION

88. (U) Accordingly, based upon my personal consideration of the matter, I have concluded that disclosure of the information described in this declaration could be expected to risk circumvention of the law and cause harm to national security. Thus, this information is properly protected from disclosure by the law enforcement privilege.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 23rd day of April 2018.

Timothy P. Groh
Deputy Director for Operations
Terrorist Screening Center

U) ~~LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of the TSC/FBI and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without the TSC/FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website or an unclassified network.~~

(U) Warning: ~~This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need-to-know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.~~